I CLAIM:

1. A computer-implemented method for providing security to a remote computer over a network browser interface, comprising:

selectively securely erasing a file associated with the remote computer, such that data associated with the file is substantially unrecoverable;

selectively scanning the remote computer to determine whether a monitoring application is present on the remote computer; and

selectively clearing activities of a user of the remote computer, such that the activities are substantially undeterminable, wherein downloading software onto the remote computer is avoided.

2. The computer-implemented method of claim 1, wherein the steps of selectively securely erasing the file, selectively scanning the remote computer, and selectively clearing activities of the user are selected to occur according to a selection made by the user.

3. The computer-implemented method of claim 1, wherein the steps of selectively securely erasing the file, selectively scanning the remote computer, and selectively clearing activities of the user are selected to occur by a security application in accordance with a user profile.

4. The computer-implemented method of claim 1, wherein selectively securely erasing the file further comprises renaming the file to a generic file name.

5. The computer-implemented method of claim 1, wherein selectively securely erasing the file further comprises overwriting data associated with the file with a sequence of data.

6. The computer-implemented method of claim 5, wherein selectively securely erasing the file further comprises determining whether additional passes of

overwriting the data associated with the file are necessary after the data associated with the file is overwritten with the sequence of data.

7. The computer-implemented method of claim 1, wherein selectively securely erasing the file further comprises providing the user functionality for dragging and dropping a file into a secure recycle bin.

8. The computer-implemented method of claim 1, wherein selectively scanning the remote computer further comprises determining whether an application associated with the remote computer is a suspect monitoring application.

9. The computer-implemented method of claim 1, wherein selectively scanning the remote computer further comprises comparing an application associated with the remote computer to a database containing descriptions of known monitoring applications.

10. The computer-implemented method of claim 1, wherein selectively scanning the remote computer further comprises alerting the user to the presence of a monitoring application when a monitoring application is found on the remote computer.

11. The computer-implemented method of claim 1, wherein selectively scanning the remote computer further comprises transmitting information about a suspect monitoring application to a server across a network when a determination is made that the suspect monitoring application is a monitoring application that is previously unidentified.

12. The computer-implemented method of claim 1, wherein selectively scanning the remote computer further comprises removing monitoring applications discovered to be present on the remote computer.

13. The computer-implemented method of claim 1, wherein selectively scanning the remote computer further comprises removing monitoring applications discovered on the remote computer.

14. A computer-readable medium encoded with computer-executable instructions for performing a method comprising:

providing a web site by which a user of the remote computer accesses a security application associated with a server, wherein the security application provides security to a remote computer over a network browser interface;

securely erasing a file associated with the remote computer when a secure erasing option that is associated with the security application is selected, such that data associated with the file is substantially unrecoverable;

scanning the remote computer to determine whether a monitoring application is present on the remote computer when a security scanning option that is associated with the security application is selected; and

clearing activities of the user of the remote computer when an activity clearing option that is associated with the security application is selected, such that the activities are substantially undeterminable by another utility, wherein downloading software onto the remote computer is avoided.

15. The computer-readable medium of claim 14, wherein securely erasing the file further comprises renaming the file to a generic file name and overwriting data associated with the file with a sequence of data.

16. The computer-readable medium of claim 14, wherein securely erasing the file further comprises providing the user functionality for dragging and dropping a file into a secure recycle bin.

17. The computer-readable medium of claim 14, wherein scanning the remote computer further comprises:

alerting the user to the presence of a monitoring application when a monitoring application is found on the remote computer;

transmitting information about a suspect monitoring application to a server across a network when a determination is made that the suspect monitoring application is a monitoring application that is previously unidentified; and

removing monitoring applications discovered to be present on the remote computer.

18. A system for providing security to a remote computer over a network browser interface, comprising:

a web site by which a user of the remote computer accesses a security application;

a security application that includes instructions for performing a method comprising:

selectively securely erasing a file associated with the remote computer, such that data associated with the file is substantially unrecoverable;

selectively scanning the remote computer to determine whether a monitoring application is present on the remote computer; and

selectively clearing activities of the user of the remote computer, such that the activities are substantially undeterminable, wherein downloading software onto the remote computer is avoided.

19. The system of claim 18, wherein selectively securely erasing the file further comprises renaming the file to a generic file name and overwriting data associated with the file with a sequence of data.

20. The system of claim 18, wherein selectively scanning the remote computer further comprises:

alerting the user to the presence of a monitoring application when a monitoring application is found on the remote computer;

transmitting information about a suspect monitoring application to a server across a network when a determination is made that the suspect monitoring application is a monitoring application that is previously unidentified; and removing monitoring applications discovered to be present on the remote computer.